

2023 -- H 5296

LC000478

STATE OF RHODE ISLAND

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2023

A N A C T

RELATING TO CRIMINAL PROCEDURE -- ELECTRONIC INFORMATION AND DATA  
PRIVACY ACT

Introduced By: Representatives Place, Rea, and Nardone

Date Introduced: February 01, 2023

Referred To: House Judiciary

It is enacted by the General Assembly as follows:

1 SECTION 1. Title 12 of the General Laws entitled "CRIMINAL PROCEDURE" is hereby  
2 amended by adding thereto the following chapter:

3 CHAPTER 34

4 ELECTRONIC INFORMATION AND DATA PRIVACY ACT

5 **12-34-1. Short title.**

6 This chapter shall be known and may be cited as the "Electronic Information and Data  
7 Privacy Act".

8 **12-34-2. Definitions.**

9 As used in this chapter:

10 (1) "Electronic communication service" means a service that provides to users of the  
11 service the ability to send or receive wire or electronic communications.

12 (2) "Electronic device" means a device that enables access to or use of an electronic  
13 communication service, remote computing service, or location information service.

14 (3) "Electronic information or data" means information or data including a sign, signal,  
15 writing, image, sound or intelligence of any nature transmitted or stored in whole or in part by a  
16 wire, radio, electromagnetic, photo-electronic, or photo-optical system:

17 (i) "Electronic information or data" includes the location information, stored data, or  
18 transmitted data of an electronic device;

1 (ii) "Electronic information or data" does not include:  
2 (A) A wire or oral communication;  
3 (B) A communication made through a tone-only paging device; or  
4 (C) Electronic funds transfer information stored by a financial institution in a  
5 communications system used for the electronic storage and transfer of money.

6 (4) "Law enforcement agency" means an entity of the state or a political subdivision of the  
7 state including any municipality within the state, or any agency acting on their behalf, that exists  
8 primarily to prevent, detect, or prosecute crime and enforce criminal statutes or ordinances.

9 (5) "Location information" means information obtained by means of a tracking device,  
10 concerning the location of an electronic device that, in whole or in part, is generated or derived  
11 from or obtained from the operation of an electronic device.

12 (6) "Location information service" means the provision of a global positioning service or  
13 other mapping, location, or directional information service.

14 (7) "Oral communication" means any oral communication uttered by a person exhibiting  
15 an expectation that the communication is not subject to interception under circumstances justifying  
16 that expectation.

17 (8) "Remote computing service" means the provision to the public of computer storage or  
18 processing services by means of an electronic communication system.

19 (9) "Transmitted data" means electronic information or data that is transmitted wirelessly  
20 from:

21 (i) An electronic device to another electronic device without the use of an intermediate  
22 connection or relay; or

23 (ii) An electronic device to a nearby antenna.

24 (10) "Wire communications" means any aural transfer made in whole or in part through  
25 the use of facilities for the transmission of communications by the aid of wire, cable, or other like  
26 connection between the point of origin and the point of reception, (including the use of the  
27 connection in a switching station) furnished or operated by any person engaged in providing or  
28 operating the facilities for the transmission of communications. The term includes any electronic  
29 storage of the communication.

30 **12-34-3. Electronic information or data privacy-Warrant required for disclosure.**

31 (a) Except as provided in subsection (e) of this section, for a criminal investigation or  
32 prosecution, a law enforcement agency shall not obtain the following electronic information or  
33 data, without a search warrant issued by a court upon a finding of probable cause:

34 (1) The location information, stored data, or transmitted data of an electronic device; or

1           (2) Electronic information or data transmitted by the owner of the electronic information  
2 or data to a remote computing service provider.

3           (b) Except as provided in subsection (d) of this section, a law enforcement agency shall not  
4 use, copy, or disclose, for any purpose, the location information, stored data, transmitted data of an  
5 electronic device, or electronic information or data provided by a remote computing service  
6 provider, that:

7                 (1) Is not the subject of the warrant; and

8                 (2) Is collected as part of an effort to obtain the location information, stored data,  
9 transmitted data of an electronic device, or electronic information or data provided by a remote  
10 computing service provider that is the subject of the warrant described in subsection (a) of this  
11 section.

12           (c) A law enforcement agency may use, copy, or disclose the transmitted data of an  
13 electronic device used to communicate with the electronic device that is the subject of the warrant,  
14 if the law enforcement agency reasonably believes that the transmitted data is necessary to achieve  
15 the objective of the warrant.

16           (d) The electronic information or data described in subsection (b) of this section shall be  
17 destroyed in an unrecoverable manner by the law enforcement agency as soon as reasonably  
18 possible after the electronic information is collected.

19           (e) A law enforcement agency may obtain location information without a warrant for an  
20 electronic device:

21                 (1) If the device is reported stolen by the owner;

22                 (2) With the informed, affirmative consent of the owner or user of the electronic device;

23                 (3) In accordance with a judicially recognized exception to the warrant requirement;

24                 (4) If the owner has voluntarily and publicly disclosed the location information; or

25                 (5) From the remote computing service provider, if the remote computing service provider  
26 voluntarily discloses the location information:

27                     (i) Under a belief that an emergency exists involving an imminent risk to an individual of  
28 death, serious physical injury, sexual abuse, live-streamed sexual exploitation, kidnapping, or  
29 human trafficking; or

30                     (ii) That is inadvertently discovered by the remote computing service provider and appears  
31 to pertain to the commission of a felony, or of a misdemeanor involving physical violence, sexual  
32 abuse, or dishonesty.

33           (f) A law enforcement agency may obtain stored or transmitted data from an electronic  
34 device, or electronic information or data transmitted by the owner of the electronic information or

1 data to a remote computing service provider, without a warrant:

2 (1) With the informed consent of the owner of the electronic device or electronic  
3 information or data;

4 (2) In accordance with a judicially recognized exception to the warrant requirement;

5 (3) In connection with a report forwarded by the National Center for Missing and Exploited  
6 Children under 18 U.S.C. § 2258A; or

7 (4) From the remote computing service provider, if the remote computing service provider  
8 voluntarily discloses the location information:

9 (i) Under a belief that an emergency exists involving an imminent risk to an individual of  
10 death, serious physical injury, sexual abuse, live-streamed sexual exploitation, kidnapping, or  
11 human trafficking; or

12 (ii) That is inadvertently discovered by the remote computing service provider and appears  
13 to pertain to the commission of a felony, or of a misdemeanor involving physical violence, sexual  
14 abuse, or dishonesty.

15 (g) A prosecutor may obtain a judicial order based on a finding of probable cause,  
16 consistent with 18 U.S.C. §§ 2703 and 2702(b) and (c), to the electronic communications system  
17 or service or remote computing service provider that owns or controls the Internet protocol address,  
18 websites, email address, or service to a specific telephone number, requiring the production of the  
19 following information, if available, upon providing in the court order the Internet protocol address,  
20 email address, telephone number, or other identifier, and the dates and times the address, telephone  
21 number, or other identifier suspected of being used in the commission of the offense;

22 (1) Names of subscribers, service customers, and users;

23 (2) Addresses of subscribers, service customers, and users;

24 (3) Records of session times and durations;

25 (4) Length of service, including the start date and types of service utilized; and

26 (5) Telephone or other instrument subscriber numbers or other subscriber identifiers,  
27 including any temporarily assigned network address.

28 (h) An electronic communication service provider or remote computing service provider,  
29 their officers, agents, employees or other specified individuals acting pursuant to and in accordance  
30 with the provisions of this chapter, may not be held liable for providing information, facilities, or  
31 assistance in good faith reliance on the terms of the warrant or without a warrant in accordance  
32 with subsections (e) and (f) of this section.

33 (i) Nothing in this chapter affects the provisions of chapter 2 of title 38, (access to public  
34 records act,) or limits or affects the rights of an employer to voluntarily provide location

1 information, stored or transmitted data from an electronic device, or electronic information or data  
2 transmitted by an employee utilizing an electronic device owned by the employer.

3 **12-34-4. Notification required - Delayed notification.**

4 (a) Except as provided in subsection (b) of this section, a law enforcement agency that  
5 executes a warrant pursuant to this chapter shall, within fourteen (14) days after the day on which  
6 the electronic information or data that is the subject of the warrant is obtained by the law  
7 enforcement agency, issue a notification to the owner of the electronic device or electronic  
8 information or data specified in the warrant that includes the following information:

9 (1) That a warrant was applied for and granted;

10 (2) The kind of warrant issued;

11 (3) The period of time during which the collection of the electronic information or data was  
12 authorized;

13 (4) The offense specified in the application for the warrant;

14 (5) The identity of the law enforcement agency that filed the application; and

15 (6) The identity of the judge or magistrate who issued the warrant.

16 (b) The notification requirement of subsection (a) of this section, shall not be triggered  
17 until the owner of the electronic device or electronic information or data specified in the warrant is  
18 known, or could reasonably be identified, by the law enforcement agency.

19 (c) A law enforcement agency seeking a warrant pursuant to this chapter may submit a  
20 request, and the court may grant permission, to delay notification required by subsection (a) of this  
21 section for a period not to exceed thirty (30) days, if the court determines that there is reasonable  
22 cause to believe that the notification may:

23 (1) Endanger the life or physical safety of an individual;

24 (2) Cause a person to flee from prosecution;

25 (3) Lead to the destruction of evidence;

26 (4) Intimidate a potential witness; or

27 (5) Otherwise seriously jeopardize an investigation or unduly delay a trial.

28 (d) When a delay of notification is granted under subsection (c) of this section and upon  
29 application by the law enforcement agency, the court may grant additional extensions of up to thirty  
30 (30) days each.

31 (e) Notwithstanding subsection (d) of this section, when a delay of notification is granted  
32 under subsection (c) of this section, and upon application by a law enforcement agency, the court  
33 may grant an additional extension of up to sixty (60) days if the court determines that a delayed  
34 notification is justified because the investigation involving the warrant:

1 (1) Is interstate in nature and sufficiently complex; or  
2 (2) Is likely to extend up to or beyond an additional sixty (60) days.

3 (f) Upon expiration of the period of delayed notification granted under subsections (c) or  
4 (d) of this section, the law enforcement agency shall serve upon or deliver by first-class mail, or by  
5 other means if delivery is impracticable, to the owner of the electronic device or electronic  
6 information or data a copy of the warrant together with notice that:

- 7 (1) States with reasonable specificity the nature of the law enforcement inquiry including:  
8 (i) The information described in subsection (a) of this section;  
9 (ii) A statement that notification of the search was delayed;  
10 (iii) The name of the court that authorized the delay of notification; and  
11 (iv) A reference to the provision of this chapter that allowed the delay of notification.

12 (g) A law enforcement agency is not required to notify the owner of the electronic device  
13 or electronic information or data if the owner is located outside of the United States.

14 **12-34-5. Third-party electronic information or data.**

15 (a) As used in this section, "subscriber record" means a record or information of a provider  
16 of an electronic communication service or remote computing service that reveals the subscriber's  
17 or customer's:

- 18 (1) Name;  
19 (2) Address;  
20 (3) Local and long distance telephone connection record, or record of session time and  
21 duration;  
22 (4) Length of service, including the start date;  
23 (5) Type of service used;  
24 (6) Telephone number, instrument number, or other subscriber or customer number or  
25 identification, including a temporarily assigned network address; and  
26 (7) Means and source of payment for the service, including credit card or bank account  
27 numbers.

28 (b) Except for purposes of grand jury testimony or use at trial after indictment, a law  
29 enforcement agency shall not obtain, use, copy or disclose a subscriber record.

30 (c) A law enforcement agency shall not obtain, use, copy or disclose, for a criminal  
31 investigation or prosecution, any record or information, other than a subscriber record, of a provider  
32 of an electronic communication service or remote computing service related to a subscriber or  
33 customer without a warrant.

34 (d) Notwithstanding subsections (b) and (c) of this section, a law enforcement agency may

1 obtain, use, copy or disclose a subscriber record, or other record or information related to a  
2 subscriber or customer, without a warrant:

3 (1) With the informed, affirmed consent of the subscriber or customer;  
4 (2) In accordance with a judicially recognized exception to warrant requirements;  
5 (3) If the subscriber or customer voluntarily discloses the record in a manner that is publicly  
6 accessible; or

7 (4) If the provider of an electronic communication service or remote computing service  
8 voluntarily discloses the record:

9 (i) Under a belief that an emergency exists involving the imminent risk to an individual of:

10 (A) Death;  
11 (B) Serious physical injury;  
12 (C) Sexual abuse;  
13 (D) Live-streamed sexual exploitation;  
14 (E) Kidnapping; or  
15 (F) Human trafficking;

16 (ii) That is inadvertently discovered by the provider, if the record appears to pertain to the  
17 commission of:

18 (A) A felony; or  
19 (B) A misdemeanor involving physical violence, sexual abuse or dishonesty; or  
20 (iii) Subject to subsection (d) of this section, as otherwise permitted under 18 U.S.C. §  
21 2702.

22 (e) A provider of an electronic communication service or remote computing service, or the  
23 provider's officers, agents, or other specified persons shall not be held liable for providing  
24 information facilities, or assistance in good faith reliance on the terms of a warrant issued under  
25 this section, or without a warrant in accordance with subsection (d) of this section.

26 **12-34-6. Exclusion of records.**

27 All electronic information or data and records of a provider of an electronic communication  
28 service or remote computing service pertaining to a subscriber or customer that are obtained in  
29 violation of the provisions of this chapter shall be subject to the rules governing exclusion as if the  
30 records were obtained in violation of the Fourth Amendment to the United States Constitution and  
31 Article 1, Section 6 of the Rhode Island Constitution.

1 SECTION 2. This act shall take effect upon passage.

=====  
LC000478  
=====



EXPLANATION  
BY THE LEGISLATIVE COUNCIL  
OF  
A N A C T  
RELATING TO CRIMINAL PROCEDURE -- ELECTRONIC INFORMATION AND DATA  
PRIVACY ACT

\*\*\*

1           This act would require law enforcement agencies to obtain search warrants for electronic  
2 information, data, location information and other identifying information of subscribers and  
3 customers, except in specified circumstances.

4           This act would take effect upon passage.

=====  
LC000478  
=====